A UNIVERSAL FORMULA FOR THE j-INVARIANT OF THE CANONICAL LIFTING

Altan Erdoğan*

November 21, 2012

Abstract

We study the j-invariant of the canonical lifting of an elliptic curve as a Witt vector. We prove that its Witt coordinates lie in an open affine subset of the j-line provided that the characteristic is at least 5 and deduce the existence of a universal formula for the j-invariant of the canonical lifting. It is also proved that a similar result holds for $p = 2, 3$ if we replace the j-line by some radiciel extension of it. The canonical liftings of the elliptic curves with j-invariant 0 and 1728 over any characteristic are also explicitly found.

1 Introduction

Let k be an algebraically closed field of characteristic p and $W(k)$ be the ring of p-typical Witt vectors of k. Let E be an ordinary elliptic curve over k. A consequence of the Serre-Tate theorem is that up to isomorphism there exists a unique elliptic curve $\mathbb{E}$ over $W(k)$

*Sponsored by TÜBİTAK

satisfying some certain conditions whose reduction modulo p is isomorphic to E. Throughout the paper we will give the definition and other properties of the canonical lifting. By definition, the j-invariant of $\mathbb{E}$, denoted by $j(\mathbb{E}) \in W(k)$ depends only on the j-invariant of E, say j_0. If we set $k^{\text{ord}} = \{j_0 \in k |$ elliptic curves with j-invariant j_0 are ordinary$\}$, we can define the following function;

$$\begin{aligned} \Theta : k^{\text{ord}} &\longrightarrow W(k), \\ j_0 &\longmapsto j(\mathbb{E}) = (j_0, j_1, ...) \end{aligned}$$

where $\mathbb{E}$ is the canonical lifting of E and each j_i is a function of j_0. The question of finding the canonical lifting in this form was first given in [7]. Here we will prove the following theorem.

Theorem A. *Let J be an indeterminate and p be any prime. Let $\phi_p(J)$ denote the* Hasse polynomial*, i.e. the polynomial in $\mathbb{F}_p[J]$ whose roots are the supersingular j-values in characteristic p. Let*

$$R = \mathbb{F}_p \left[J, \frac{1}{J(J-1728)\phi_p(J)} \right], \quad R' = R[\{J^{1/p^n}\}_{n \in \mathbb{Z}}].$$

(i) *There exist $f_i \in R'$ for all $i \in \mathbb{Z}_{\geq 1}$ such that for any $j_0 \in k^{ord} \setminus \{0, 1728\}$,*

$$\Theta(j_0) = (j_0, f_1(j_0), f_2(j_0), ...f_n(j_0), ...)$$

where we see $f_i \in R'$ as the unique homomorphism $f_i : R' \longrightarrow \overline{\mathbb{F}_p}$ extending the $\mathbb{F}_p$-algebra homomorphism

$$R \longrightarrow \overline{\mathbb{F}_p}, \quad J \longmapsto j_0.$$

(ii) *If $p \geq 5$, then $f_i \in R$ for all $i \in \mathbb{Z}_{\geq 1}$.*

(iii) *If $j_0 = 0$ is an ordinary j-value then $\Theta(0) = (0, 0, 0...)$, and similarly if $j_0 = 1728$ is an ordinary j-value then $\Theta(1728) = (1728, 0, 0, ...)$.*

The first and the second assertions of the theorem mean that we have a universal formula for the j-invariant of the canonical lifting, and if $p \geq 5$ then this universal formula is almost a polynomial. The third assertion is independent of the others and proved with a different argument.

We proceed as follows. In §2 we give a brief overview of the Serre-Tate theorem. In §3, we generalize the notion of the canonical lifting for elliptic curves defined over $\mathbb{F}_p$-schemes satisfying certain hypotheses. In §4 we use the construction given in [5] to prove that the canonical lifting of an ordinary elliptic curve over an imperfect field of characteristic $p \geq 5$ is defined over the Witt ring of this imperfect field. This result first appeared in [2], but here we give a different proof. Finally in the last section we apply the results of §3 and §4 to a universal family of ordinary elliptic curves to prove (i) and (ii) of Theorem A. We also prove (iii) in this last section.

We fix the following notation. For any schemes X/T and U/T we set $X_U := X \times_T U$. If $U = \operatorname{Spec} C$ is affine, we may use X_C instead of X_U. If $T = \operatorname{Spec} B$ is also affine, we may also use $X \otimes_B C$ for X_U. For $t \in T$ with residue field $\kappa(t)$, we denote $X \times_T \operatorname{Spec} \kappa(t)$ by X_t. For any group scheme G/T, $G[N]$ denotes the kernel of the multiplication by N on G.

Acknowledgement

I would like to thank my advisor Sinan Ünver for his invaluable support and comments at every step of my PhD research and this paper and Brian Conrad for his invaluable suggestions regarding this paper.

2 An overview of the Serre-Tate theorem

In this section we briefly recall some aspects of the Serre-Tate theorem. We restrict ourselves to the definition and a well known equivalent characterization of the canonical lifting which are directly used in the proofs. General references for a complete proof and a detailed analysis of the Serre-Tate theorem are [5] and [8]. For the sake of completeness we quote the following theorem from [5] and call it as the *general Serre-Tate theorem.*

Theorem. *Let A be a ring in which p is nilpotent. Let I be a nilpotent ideal of A, and put $A_0 = A/I$. Let* $\mathrm{AS}(A)$ *denote the category of abelian schemes over A, and let* $\mathrm{Def}(A, A_0)$ *denote the category of triples (X_0, L, ϵ) where X_0 is an abelian scheme over A_0, L is a p-divisible group over A and $\epsilon : L_0 := L \otimes_A A_0 \longrightarrow A_0[p^\infty]$ is an isomorphism. Then the functor*

$$X \longmapsto (X_0, X[p^\infty], \text{the natural map})$$

is an equivalence of the categories $\mathrm{AS}(A)$ *and* $\mathrm{Def}(A, A_0)$.

Let k be an algebraically closed field of characteristic $p > 0$ and A be an Artin local ring with residue field k. In general we say that a scheme $\mathbb{X} \longrightarrow \operatorname{Spec} A$ lifts a given scheme $X \longrightarrow \operatorname{Spec} k$, if $\mathbb{X} \otimes_A k \xrightarrow{\sim} X$. Given an ordinary abelian variety X over k, the Serre-Tate theorem classifies all abelian schemes defined over A that lift X. For such an ordinary abelian variety $X \longrightarrow \operatorname{Spec} k$ and an abelian scheme $\mathbb{X} \longrightarrow \operatorname{Spec} A$ lifting X/k, there are the associated p-divisible groups (= Barsotti-Tate groups) denoted by $X[p^\infty]$ and $\mathbb{X}[p^\infty]$ respectively which play an important role summarized in the following diagram;

$$\begin{aligned}
\{\text{Isomorphism classes of } \mathbb{X}/A \text{ lifting } X/k\} &\xrightarrow{\sim} \\
\{\text{Isomorphism classes of } \mathbb{X}[p^\infty]/A \text{ lifting } X[p^\infty]/k\} &\xrightarrow{\sim} \\
\mathrm{Ext}_A(T_p(X)(k)\otimes \mathbb{Q}_p/\mathbb{Z}_p, \mathrm{Hom}_{\mathbb{Z}_p}(T_p(X^D)(k), \hat{\mathbb{G}}_m) &\xrightarrow{\sim} \\
\mathrm{Hom}_{\mathbb{Z}_p}(T_p(X)(k)\otimes T_p(X^D)(k), \hat{\mathbb{G}}_m(A)),&
\end{aligned}$$

where $T_p(X)(k)$ is the Tate module of X, X^D denotes the dual abelian variety, $\hat{\mathbb{G}}_m$ denotes the formal completion of the multiplicative group $\mathbb{G}_m$ and $\mathrm{Ext}_A(-,-)$ denotes the extension group of A-groups. General references for the properties of p-divisible groups are [11] and [8]. The above diagram shows that the set

$$\{\text{Isomorphism classes of } \mathbb{X}/A \text{ lifting } X/k\}$$

has a natural group structure.

Definition. *With the above notation the unique abelian scheme $\mathbb{X}/A$ which corresponds to the identity element of the group*

$$\mathrm{Ext}_A(T_p(X)(k)\otimes \mathbb{Q}_p/\mathbb{Z}_p, \mathrm{Hom}_{\mathbb{Z}_p}(T_p(X^D)(k), \hat{\mathbb{G}}_m))$$

is called the canonical lifting of X/k over A.

Remark. In the introduction, the base of the canonical lifting is given to be a characteristic zero integral domain, but here we define it over an Artin local ring which indeed fits well to our purposes. At the end of this section we will see that this definition is justified.

Remark 1. If we only assume that k is perfect than the above diagram and the definition still remain valid by a slight change of the objects involved. A complete study of equivalent definitions of the canonical lifting for perfect k can be found in [8, V.3 and the Appendix].

Equivalently the canonical lifting of X/k over A can be defined as the unique abelian scheme with a trivial "Serre-Tate q-parameter"

$$q(= q_{\mathbb{X}/A}) \in \mathrm{Hom}_{\mathbb{Z}_p}(T_p(X)(k) \otimes T_p(X^D)(k), \hat{\mathbb{G}}_m(A)).$$

We will use this fact in §4, but first we need to manipulate it to be able to use in the way we want. Again the details can be found in [5]. Let I be the maximal ideal of A and r be a sufficiently large integer such that $I^r = 0$. Let $\mathbb{X}/A$ be any lifting of X/k. Then we have the following perfect pairing

$$E_{\mathbb{X}} : \hat{\mathbb{X}} \times T_p(X^D)(k) \longrightarrow \mathbb{G}_m.$$

and the homomorphism

$$\begin{aligned} \phi_r : X(k)[p^r] &\longrightarrow \hat{\mathbb{X}}(A) \\ P &\longmapsto p^r(\hat{P}) \end{aligned}$$

where $\hat{P} \in \hat{\mathbb{X}}(A)$ is any lifting of P. Also the composition $\phi_{\mathbb{X}} : T_p(X)(k) \twoheadrightarrow X(k) \to \hat{\mathbb{X}}(A)$ is well-defined, i.e. ϕ_r is compatible with the map $p : X(k)[p^{r+1}] \longrightarrow X(k)[p^r]$. Then $q = q_{\mathbb{X}/A}$ is defined as $q(\alpha, \beta) := E_{\mathbb{X}}(\phi_{\mathbb{X}}(\alpha), \beta)$. Since the pairing $E_{\mathbb{X}}$ is perfect, q is trivial if and only if $\phi_{\mathbb{X}}$ is identically equal to the identity element of the group $\mathbb{X}(A)$, say O. This is equivalent to saying that $p^r(\hat{P}) = O$ for any $P \in X(k)[p^r]$. If in addition X is an elliptic curve, then $X = X^D$ and the group $X[p^r](k)$ is cyclic, so it is enough to show that $p^r(\hat{P}) = O$ for some generator $P \in X(k)[p^r]$. Hence we have the following equivalent condition for $\mathbb{X}/A$ to be the canonical lifting of X/k:

For some generator $P \in X[p^r](k)$ and for some $\hat{P} \in \mathbb{X}(A)$ lifting P, $p^r(\hat{P}) = O$. (2.1)

The particular case we are concerned with here is the case where $A = W_n(k)$, the ring of p-typical Witt vectors of length n. Recall that if k is a perfect field of characteristic p then $W_n(k)$ is an Artin local ring with residue field k and maximal ideal (p). See [9] for the definition and basic facts about Witt vectors which we use here. In this case the canonical liftings $\mathbb{X}_m/W_m(k)$ are compatible with each other, i.e. for any $m \leq n$,

$$\mathbb{X}_n \otimes_{W_n(k)} W_m(k) \xrightarrow{\sim} \mathbb{X}_m.$$

Thus the inverse system $(\mathbb{X}_m/W_m(k))_m$ defines a formal abelian variety over $W(k)$ which can be algebraicized ([8], §V.3.3). This abelian variety is defined as the canonical lifting of X/k over $W(k)$, and hence justifies our definition above. If there is no confusion about the base we will just say the canonical lifting of X/k.

3 Canonical lifting of families

In this section we will show that we can extend the definition of the canonical lifting to elliptic curves defined over $\mathbb{F}_p$-schemes under some hypothesis. This will allow us to mention about the canonical lifting of a family of elliptic curves. Main result of this section is Theorem B which is stated and proved at the end of this section.

Let R be a Noetherian integral $\mathbb{F}_p$-algebra with fields of fractions K. We fix an algebraic closure of K, and denote it by $\bar{K}$. Let K' be the perfect closure of K (i.e. the maximal purely inseparable extension of K) in $\bar{K}$ and R' be the integral closure of R in K'. We also define the subrings

$$R_n = R^{1/p^n} = \{x \in \bar{K} | x^{p^n} \in R\}.$$

Note that R_n is Noetherian, and $R' = \cup_n R_n$ and the morphism of schemes $\operatorname{Spec} R' \longrightarrow \operatorname{Spec} R$ induced by the inclusion $R \hookrightarrow R'$ is a homeomorphism. If $s' \in \operatorname{Spec} R'$ maps to $s \in \operatorname{Spec} R$ then $\kappa(s')$ is the perfect closure of $\kappa(s)$ [3]. Let E/R be an ordinary elliptic curve in the sense of [6, §2 and §12]. Then Zariski locally on $\operatorname{Spec} R$, E/R will have a Weierstrass equation

$$y^2 + a_1xy + a_3x = x^3 + a_2x^2 + a_4x + a_6.$$

Explicitly there is an open affine cover $\{U_\alpha\}_{\alpha \in I}$ of $\operatorname{Spec} R$ such that each elliptic curve $E \times_{\operatorname{Spec} R} U_\alpha$ has a Weierstrass equation with coefficients in $\Gamma(U_\alpha, O_{U_\alpha})$ [6, §2.2]. Let E_n be the scheme defined as

$$y^2 + (a_1)^{1/p^n}xy + (a_3)^{1/p^n}x = x^3 + (a_2)^{1/p^n}x^2 + (a_4)^{1/p^n}x + (a_6)^{1/p^n}$$

Zariski locally on $\operatorname{Spec} R_n$. Then E_n is an elliptic curve, and indeed $E_n \xrightarrow{\sim} E \otimes_R R_n$ where the base change is done via the p^n-th root homomorphism $R \longrightarrow R_n$. Throughout this section E/R and E_n/R_n will always denote these elliptic curves defined here. To simplify notation we use E also to denote the base extensions $E \otimes_{R,i} R_n$ and $E \otimes_{R,i} R'$ where i is the inclusion map.

Now let T be the spectrum of a field or a complete Noetherian local ring. Then for any finite locally free group scheme G/T, there is a unique exact sequence with some certain universal properties

$$0 \longrightarrow G^0 \longrightarrow G \longrightarrow G^{et} \longrightarrow 0$$

called the *connected- étale sequence* of G [10]. A similar construction for p-divisible groups also exists. If $G = (G_n, i_n)_n$ is a p-divisible group, then $G^0 := (G_n^0, i_n)_n$ and $G^{et} := (G_n^{et}, i_n)_n$

are connected and étale p-divisible groups respectively. By [11] we have an exact sequence of p-divisible groups

$$0 \longrightarrow G^0 \longrightarrow G \longrightarrow G^{et} \longrightarrow 0.$$

Note that for any ordinary elliptic curve $\tilde{E}$ over a perfect field F, the sequence

$$0 \longrightarrow \tilde{E}[p^\infty]^0 \longrightarrow \tilde{E}[p^\infty] \longrightarrow \tilde{E}[p^\infty]^{et} \longrightarrow 0$$

splits over F. This fact is very crucial in the construction of the canonical lifting (Recall Remark 1). So in order to generalize the notion of the canonical lifting we need a similar result when F is replaced by another scheme. But *a priori* we don't even know that $E[p^\infty]$ has a connected- étale sequence over an arbitrary base. The following theorems of Messing which we directly quote from [8] and the Proposition 1 below allow us to overcome this problem.

Theorem 1. *Let S be any scheme and $f : X \longrightarrow S$ be a finite locally free morphism of schemes. Then the function $s \longmapsto$ (separable rank of X_s) is locally constant on S if and only if there are morphisms $i : X \longrightarrow X'$ and $f' : X' \longrightarrow S$ which are finite and locally free with i radiciel and surjective, f' étale and $f = f' \circ i$. The factorization is unique up to unique isomorphism and is functorial in X/S.*

Proof. [8, §II.4.8]. □

Theorem 2. *Let S be a scheme on which p is locally nilpotent, and G be a p-divisible group over S. Then the following conditions are equivalent.*

1. *$\overline{G}$ is a p-divisible group over S (For the definition of $\overline{G}$, see [8, §II]).*
2. *G is an extension of an étale p-divisible group G^{et} by a connected p-divisible group G^0.*

3. *G is an extension of an étale p-divisible group G^{et} by a p-divisible formal Lie group Γ.*

4. *For all n, $G[p^n]$ is an extension of a finite étale group by a finite locally free radiciel group.*

5. *$G(1)$ is an extension of a finite étale group by a finite locally free radiciel group.*

6. *The function $s \longmapsto$ (separable rank of $G[p]_s$) is locally constant on S.*

Proof. [8, §II.4.9] □

Proposition 1. *Let $E[p^n]$ denote the kernel of $p^n : E \longrightarrow E$ and $E[p^\infty]$ be the p-divisible group of E.*

(i) *For each n there is a unique connected- étale sequence*

$$0 \longrightarrow E[p^n]^0 \longrightarrow E[p^n] \longrightarrow E[p^n]^{et} \longrightarrow 0$$

which splits over R_n.

(ii) *There is a unique connected- étale sequence of p-divisible groups*

$$0 \longrightarrow E[p^\infty]^0 \longrightarrow E[p^\infty] \longrightarrow E[p^\infty]^{et} \longrightarrow 0,$$

which splits over R'.

Proof. By hypothesis E is ordinary, so the p-divisible group $G = E[p^\infty]$ satisfy the last condition of Theorem 2, and the existence of both sequences follow. Recall the notation we adopted for E, i.e. we can take the base to be R, R_n or R' and so we have the relevant connected- étale sequences over any of these bases. But by the uniqueness assertion of Theorem 1 these sequences are compatible with each other in the sense that $E_{R'}[p^n]^0 =$

$(E[p^n]^0)_{R'}$ and similarly for other groups and the other base R_n. Thus the uniqueness of the sequences in the theorem also follow.

The remaining thing is to prove the splitting of the sequences over the specified bases. First note that the splitting of the sequences given in (i) for all n imply the splitting of the sequence given in (ii). Thus we only need to show that

$$0 \longrightarrow E[p^n]^0 \longrightarrow E[p^n] \longrightarrow E[p^n]^{et} \longrightarrow 0$$

splits over R_n. Also the groups involved here are all commutative, so splitting amounts to giving a section of $E[p^n] \longrightarrow E[p^n]^{et}$ over R_n.

Let $F^n : \operatorname{Spec} R_n \longrightarrow \operatorname{Spec} R_n$ be the n-th iterate of the absolute Frobenius of $\operatorname{Spec} R_n$. Then we have

$$E_n^{(p^n)} := E_n \otimes_{R_n, F^n} R_n = E \otimes_{R,i} R_n (= E).$$

To simplify notation we use F^n also to denote the n-th iterate of the relative Frobenius of E_n; $F^n : E_n \longrightarrow E_n^{(p^n)}$. We denote the dual isogeny of F^n by V^n. Then we have the following commutative diagram

$$\begin{array}{ccc} E & \xrightarrow{V^n} & E_n \\ & \searrow^{[p^n]} & \downarrow{\scriptstyle F^n} \\ & & E \end{array}$$

which shows that $\ker(V^n)$ is a subgroup of $E[p^n]$. But since E is ordinary then $\ker(V^n)$ is a finite étale group over R_n [6, §12.3.6]. The inclusion $\ker(V^n) \hookrightarrow E[p^n]$ will give a required section once we can show that $\ker(V^n) \xrightarrow{\sim} E[p^n]^{et}$. Note that this isomorphism holds over algebraically closed fields; since then $E[p^n] = \mu_{p^n} \times \mathbb{Z}/p\mathbb{Z}$, and V^n is the identity on μ_{p^n}

and kills $\mathbb{Z}/p\mathbb{Z}$. Our aim is to reduce to this case. In general the composition

$$\ker(V^n) \longrightarrow E[p^n] \longrightarrow E[p^n]^{et} \tag{3.1}$$

is a group homomorphism, so necessarily commutes with the action of the étale fundamental group (see [10] for the definition of the étale fundamental group). Finally we remark that R_n is Noetherian for any n. Now the following theorem of Grothendieck completes the proof. □

Theorem. *Let S be a locally Noetherian scheme, α be a geometric point, and $\pi = \pi(S, \alpha)$ be the étale fundamental group of S centered at α. Then the functor $Y \longmapsto Y(\alpha)$ establishes an equivalence between the category of finite étale schemes over S and the category of finite sets with a continuous π action.*

Remark. The sequence given in (ii) of Proposition 1 also captures the connected- étale sequence of the fibre $\kappa(s')$ for any $s' \in \operatorname{Spec} R'$ in the following sense;

$$(E[p^\infty]^{et})_{s'} = (E_{s'}[p^\infty])^{et} \quad \text{and} \quad (E[p^\infty]^0)_{s'} = (E'_s[p^\infty])^0.$$

Now we will use Proposition 1, and the general Serre-Tate theorem to find a good lifting of $E(= E_{R'})$ to $W_m(R')$ for each m. We will need the following important theorem of Grothendieck.

Theorem 3. *Let A be a ring, I an ideal of A. Suppose that A is complete and separated with respect to topology defined by the ideal I. Put $A_0 = A/I$. Then the functor*

$$X \longmapsto X \otimes_A A_0$$

establishes an equivalence between the category of finite étale A-schemes and the category

of finite étale A_0-schemes.

Proof. [4, §18.3.2]. □

Theorem B. *Let R be a Noetherian, integral $\mathbb{F}_p$-algebra with perfect closure R', and E be an ordinary elliptic curve over R. Then for each m there exists a unique elliptic curve $\mathbb{E}_m/W_m(R')$ such that for any $s' \in \operatorname{Spec} R'$ with residue field $\kappa(s')$, the elliptic curve*

$$\mathbb{E}_m \otimes_{W_m(R')} W_m(\kappa(s'))$$

is the canonical lifting of $E_{s'}$ to $W_m(\kappa(s'))$.

Proof. Let $m \geq 2$ be a fixed integer. Since R' is a perfect ring, $A = W_m(R')$ satisfies the hypothesis of Theorem 3. So for any n there exists a unique group scheme H_n over $W_m(R')$ such that

$$H_n \otimes_{W_m(R')} R' \xrightarrow{\sim} E[p^n]^{et}.$$

It also follows that H_n form an inductive system, and so the limit gives a p-divisible group H_∞ lifting $E[p^\infty]^{et}$. Applying Cartier duality to $E[p^n]^{et}$, we see that $E[p^n]^0$ and so $E[p^\infty]^0$ has also a unique lifting G_∞ to $W_m(R')$. Since the sequence given in (ii) of Proposition 1 is split exact, the product $G_\infty \times H_\infty$ lifts the p-divisible group $E[p^\infty]$.

By the general Serre-Tate theorem there is a unique abelian scheme $\mathbb{E}_m$ over $W_m(R')$ lifting E which corresponds to $G_\infty \times H_\infty$, and so has a split exact connected- étale sequence

$$0 \longrightarrow \mathbb{E}_m[p^\infty]^0 \longrightarrow \mathbb{E}_m[p^\infty] \longrightarrow \mathbb{E}_m[p^\infty]^0 \longrightarrow 0.$$

By checking fibers or dimension we can see that $\mathbb{E}_m$ is indeed an elliptic curve.

Now by construction for any $s' \in \operatorname{Spec} R'$, the elliptic curve $\mathbb{E}_m \otimes_{W_m(R')} W_m(\kappa(s'))$

lifts $E_{s'}$ and the associated p-divisible group

$$\mathbb{E}_m[p^\infty] \otimes_{W_m(R')} W_m(\kappa(s'))$$

has a split exact connected- étale sequence. So $\mathbb{E}_m \otimes_{W_m(R')} W_m(\kappa(s'))$ must be the canonical lifting of $E_{s'}$. □

For the purposes of this paper we may call the elliptic curve $\mathbb{E}_m$ as the canonical lifting of E over $W_m(R')$. The j-invariant of $\mathbb{E}_m$, denoted by $j(\mathbb{E}_m)$ will be the universal formula for the canonical lifting of the fibers in the following sense: Let

$$j(\mathbb{E}_m) = (j_0, j_1, ..., j_{m-1})$$

and let $f_{s'} : R' \longrightarrow \kappa(s')$ be the canonical map for $s' \in \operatorname{Spec} R'$. Then the j-invariant of the canonical lifting of $E_{s'}$ to $W_m(\kappa(s'))$ is given by

$$j = (f_{s'}(j_0), f_s(j_1), ..., f_s(j_{m-1})).$$

4 Canonical lifting over imperfect fields

In this section we will use the condition 2.1 to prove that the base of the canonical lifting has a well behaviour with respect to the base of the given ordinary elliptic curve. Explicitly we will prove the following theorem.

Theorem C. *Let K be any field of characteristic $p \geq 5$, and let E be an ordinary elliptic curve over K. Let $\mathbb{E}$ be the canonical lifting of E over $W(\bar{K})$. We denote the j-invariant of $\mathbb{E}$ by $j(\mathbb{E}) = (j_0, j_1, ..., j_n, ...)$. Then each j_n is an element of K.*

The theorem holds for perfect K by definition. The interesting thing is that the canonicalness imply that it also holds for imperfect fields. This theorem was proved by Finotti, L.R.A. in [2] by using Greenberg transforms and elliptic Teichmüller lifts. Here we give a different proof.

First we make a reduction. Let K' and K^s denote the perfect and separable closures of K respectively. Then by construction of the canonical lifting $j_n \in K'$. Since $K' \cap K^s = K$ it is enough to prove that $j_n \in K^s$. Thus by changing the base to K^s we can assume K to be a separably closed field. The condition 2.1 is only about the p-th power torsion points. So we may recall and give some basic facts about the division polynomials before we go into the proof. A basic reference for division polynomials is [1]. Also we will use some basic facts about Witt vectors. The statements which we do not prove here in detail are easy consequences of results of [9, §II.4-5].

We fix K and E as in the theorem. Fix a Weierstrass model of E/K,

$$E : y_0^2 = x^3 + a_0 x_0 + b_0$$

where $a_0, b_0 \in K$.

For any odd integer N, let $\Psi_{E,N}(x)$ be the N-*division polynomial*, i.e. the polynomial in $\mathbb{Z}[a_0, b_0, x]$ whose roots are exactly the x-coordinates of the N-torsion points of $E(\bar{K})$ (For N even the division polynomial is in $\mathbb{Z}[a_0, b_0, x, y]$). In other words $\Psi_{E,N}(x_0) = 0$ for some $x_0 \in \bar{K}$ if and only if $P = (x_0, y_0) \in E(\bar{K})$ is an N-torsion point for some $y_0 \in \bar{K}$. So the only N-torsion points which can not be obtained from the roots of $\Psi_{E,N}$ are the points lying in $E[N]^0(\bar{K})$. Obviously in this case $E[N]^0(\bar{K})$ consists of only one point, but the concept of division polynomials can be generalized for any base and this observation remains true [1].

We are interested in the special case $N = p^n$ for $n \geq 1$. Consider the set

$$L_n = \{\alpha \in \bar{K} | O \neq P = (\alpha, \beta) \in E[p^n](\bar{K}) \text{ for some } \beta \in \bar{K}\}.$$

Note that $|L_n| = (p^{2n} - 1)/2$.

Since K is separably closed we have that either $L_n \subset K$ or $K(\{L_n\})$ is a purely inseparable extension of K. In the first case $\Psi_{E,p^n}(x)$ splits over K, and in the second case it is a polynomial in x^{p^l} over K for some l. A simple degree consideration shows that $l \leq n$, and so $\alpha^{p^n} \in K$ for any $\alpha \in L_n$.

Now take a general Weierstrass equation over the ring of Witt vectors lifting E;

$$A : (y_0, y_1, ...)^2 = (x_0, x_1, ...)^3 + (a_0, a_1, ...)(x_0, x_1, ...) + (b_0, b_1, ...).$$

We can see y_i, x_i, a_i, and b_i as indeterminates for $i \geq 1$. We may also see this Weierstrass equation as an equation in the variables x_i, y_i with coefficients in $W(F)$ where F is an algebraically closed field containing $\bar{K}$ and all the indeterminates a_i and b_i. So any lifting of E can be obtained by choosing $a_i, b_i \in \bar{K}$ for $i \geq 1$. The idea of the proof is that we can choose $a_i, b_i \in K$ in such a way that the obtained nonsingular cubic will be a Weierstrass model of the canonical lifting of E. We will prove it inductively on the index i of the variables $\{a_i, b_i\}$. Note that if A is the canonical lifting then $A_n := A \pmod{p^n}$ will be the canonical lifting of E over $W_n(\bar{K})$.

We introduce the following notation. Fix a positive integer n. Let

$$A_{n+1} : (y_0, ..., y_n)^2 = (x_0, ..., x_n)^3 + (a_0, ..., a_n)(x_0, ..., x_n) + (b_0, ..., b_n)$$

be the reduction of A modulo p^{n+1}. In [1], Cassels define the division polynomials $\Psi = \Psi_{C,N}$

for any positive integer N and for any cubic equation

$$C : y^2 = x^3 + Gx + H$$

where G and H are independent indeterminates. He proves that these division polynomials have integer coefficients and satisfy

$$(\Psi^2)' \equiv 0 \pmod{N},$$

where $()'$ means the derivative with respect to x. In our case since $\mathrm{char}(K) \neq 2$ this means that for any odd N, $\Psi\Psi' \in N.W_{n+1}(F)[x]$. We can state this in a different way as the following technical lemma.

Lemma 1. *The p^{n+1}-division polynomial Ψ of A_{n+1} satisfies $\Psi' = 0$ in $W_{n+1}(F)[x]$.*

Proof. Since $p^{n+1} = 0$ in $W_{n+1}(F)[x]$, $\Psi' \neq 0$ implies that Ψ is a zero divisor in the polynomial ring $W_{n+1}(F)[x]$. This can happen only if there exists a nonzero $B \in W_{n+1}(F)$ such that $B\Psi = 0$. But by construction $\Psi(\mathrm{mod}\ p) = \Psi_{E,p^n}(x)$ is not identically zero. Thus coefficients of some terms of Ψ are nonzero modulo p, i.e. units in $W_{n+1}(F)$. So $B\Psi = 0$ can occur only if $B = 0$. Thus Ψ can not be a zero divisor, and so $\Psi' = 0$. □

Now we can prove Theorem C.

Proof of Theorem C. Let

$$\Psi = \Psi_{A_{n+1},p^{n+1}} = B_l + B_{l-1}X + ... + B_1X^{l-1} + B_0X^l$$

where $B_i \in W_{n+1}(F)$ and we can see the variable X as $X = (x_0, x_1, ..., x_n)$. Indeed B_i are polynomials with integer coefficients in the variables $(a_0, a_1, ..., a_n), (b_0, b_1, ..., b_n)$. By

Lemma 1 for each monomial B_iX^{l-i} of Ψ we have that $(l-i)B_i \in (p^{n+1})$, i.e. equal to zero. Let ν_p denote the p-adic valuation of rational integers. Let $\nu_p(l-i) = p^{t_i}$ where we can assume $t_i \geq 1$ (otherwise $B_i = 0$). Then we have that $B_i \in (p^{n+1-t_i})$. Also we have

$$\begin{aligned} X^{p^{t_i}} = (x_0, x_1, ..., x_n)^{p^{t_i}} &= (x_0^{p^{t_i}}, 0, 0..., 0, y_{j+1}, y_{j+2}, ..., y_n) \\ &= (x_0^{p^{t_i}}, 0, 0..., 0) + (0, 0, 0..., 0, y_{j+1}, y_{j+2}, ..., y_n) \end{aligned}$$

where each y_i is some polynomial in $\{x_i\}_i$, j is an integer with $j \geq t_i$ and y_{j+1} is in the $(j+1)$-st index. Put $u = (x_0^{p^{t_i}}, 0, 0..., 0)$ and $\pi = (0, 0, 0..., 0, y_{j+1}, y_{j+2}, ..., y_n)$. So we have

$$B_iX^{p^{t_i}} = B_i(u + \pi) = uB_i$$

since $\pi \in (p^{t_i})$ and $B_i \in (p^{n+1-t_i})$. But $B_i = (0, 0, ..., 0, d_{i,n-t_i+1}, ...d_{i,n})$ where the first possibly nonzero term appears at the $(n - t_i + 1)$-st index. Multiplying by u we get

$$uB_i = (0, 0, ..., 0, d_{i,n-t_i+1}x_0^{p^{n+1}}, ...)$$

where any nonzero index is of the form $dx_0^{r.p^{n+1}}$ for some nonnegative integer r, and for some $d \in K[\{a_i, b_i\}_i]$. Thus Ψ is of the form

$$\Psi = (\Psi_0, \Psi_1, ..., \Psi_n)$$

where each Ψ_j is an element of $K[\{a_i, b_i\}_i, x_0^{p^{n+1}}]$ for $i \leq j$. But more than this is true; each Ψ_j is linear with respect to a_j and b_j. This directly follows from the addition and multiplication rules of Witt vectors and keeping in mind that characteristic is p.

The key ideas here are that each Ψ_j in the above notation is a polynomial in $x_0^{p^{n+1}}$ and for any $P = (x_0, y_0) \in E[p^{n+1}](\bar{K})$ we have that $x_0^{p^{n+1}} \in K$. So choosing an appropriate

$P = (x_0, y_0)$ with $x_0 \in L_n$ and forcing Ψ_j to satisfy the condition 2.1, we obtain an equation of the form

$$\alpha_j a_j + \beta_j b_j + \gamma_j = 0$$

where α_j, β_j and γ_j are polynomials in a_i, b_i for $i = 0, 1, ...j-1$. But by hypothesis E is defined over K, i.e. $a_0, b_0 \in K$, also existence of the canonical lifting guarantees that this equation has a solution probably in $\bar{K}$. So we may apply induction: In the case $j = 1$, by hypothesis the above linear equation has coefficients in K and so always have a solution $a_1, b_1 \in K$. For the induction step assume that $a_i, b_i \in K$ for $i \leq j-1$. Then we have a similar situation; a linear equation in a_j and b_j with coefficients in K. We can take any $a_j, b_j \in K$ satisfying this linear equation. So we have a Weierstrass model for the canonical lifting with $a_i, b_i \in K$ for all $i \leq n$. In particular the j-invariant of A_{n+1} lies in $W_{n+1}(K)$. But as n is arbitrary this shows that $j_n \in K$ for any $n \geq 0$. □

5 The universal formula

Now we can use the results of the previous sections to prove Theorem A stated in §1.

Proof of Theorem A. Let p be any prime number. Recall that we defined the ring R as

$$R = \mathbb{F}_p[J, 1/J(J-1728)\Phi_p(J)].$$

We define the elliptic curve E/R as

$$E : y^2 + xy = x^3 - 36x/(J-1728) - 1/(J-1728).$$

Note that $j(E) = J$ and E is ordinary. So the hypotheses of Theorem B is satisfied. With the same notation of Theorem B, for any positive integer m we have the elliptic curve $\mathbb{E}_m$ over $W_m(R')$ with j-invariant $j(\mathbb{E}_m) = (j_0, j_1, j_2, ..., j_m)$. Now for any $j_0 \in k^{\text{ord}} \setminus \{0, 1728\}$, the homomorphism $R' \longrightarrow \overline{\mathbb{F}_p}$ induced by $J \longmapsto j_0$ maps E to an ordinary elliptic curve over $\overline{\mathbb{F}_p}$ with j-invariant j_0, say $\tilde{E}$. Similarly it maps $\mathbb{E}_m$ to the canonical lifting of $\tilde{E}$. Thus the proof of (i) is complete once we set $j_i = f_i$ for all i.

Now assume $p \geq 5$ and let K and K' be the fields of fractions of R and R' respectively. Consider the elliptic curve

$$\mathbb{E}_m \otimes_{W_m(R')} W_m(K')$$

obtained via the inclusion $W_m(R') \hookrightarrow W_m(K')$. It is a lifting of the generic fiber of E denoted by $E_{K'} = E \otimes_{R'} K'$ and has a split exact connected- étale sequence over $W_m(K')$. So it is the canonical lifting of $E_{K'}$. Its j-invariant is in $W_m(R')$ as it is obtained from $\mathbb{E}_m$. But E is indeed defined over K, and since $p \geq 5$ it is isomorphic to an elliptic curve

$$C : y^2 = x^3 + gx + h$$

for some $g, h \in K$. But then Theorem C implies that the j-invariant of the canonical lifting of C which is necessarily equal to the j-invariant of $\mathbb{E}_m \otimes_{W_m(R')} W_m(K')$ is indeed in $W_m(K)$. So each $j_i \in R' \cap K = R$, and this completes the proof of (ii).

Now we prove (iii). Since $J = 0 = 1728$ is supersingular for $p = 2, 3$, we may assume that $p \geq 5$. Let E be any ordinary elliptic curve over a finite field k with $j(E) = j_0 \in k$, and let $\mathbb{E}$ be its canonical lifting over $W(k)$. Then by [8, §V.3] we have that

$$\text{End}(\mathbb{E}) \xrightarrow{\sim} \text{End}(E)$$

via the reduction modulo p map. Now take any p such that $j_0 = 0$ is an ordinary j-value in $k = \mathbb{F}_p$. Then the automorphism group of $E/\mathbb{F}_p$, say $\mathrm{Aut}_{\bar{k}}(E)$ has order 6. Then by the above isomorphism we also have that $\mathrm{Aut}_{\overline{\mathbb{Q}_p}}(\mathbb{E} \otimes \overline{\mathbb{Q}_p})$ has order at least 6. But this can happen if and only if $j(\mathbb{E}) = 0$, i.e. in Witt vector notation $\Theta(0) = (0, 0, 0...)$. Similarly if E/k with $j(E) = j_0 = 1728$ is ordinary for some p, then we have that $\mathrm{Aut}_{\bar{k}}(E)$ has order 4. So that $j(\mathbb{E}) = 1728$, i.e. $\Theta(1728) = (1728, 0, 0...)$. □

References

[1] J. W. S. Cassels. A Note on the Division Values of $\wp(u)$, *Mathematical Proceedings of the Cambridge Philosophical Society*, 45(2): 167-172, 1949.

[2] L. R. A. Finotti. Lifting the j-Invariant: Questions of Mazur and Tate, *Journal of Number Theory*, 130(3): 620-638, 2010.

[3] M. J. Greenberg. Perfect Closure of Rings and Schemes, *Proc. Amer. Math. Soc.*, 16: 313-317, 1965.

[4] A. Grothendieck. EGA IV. Étude locale des schémas et des morphismes de schémas. *Inst. Hautes Études Sci. Publ. Math.*, 32, 1967.

[5] N. Katz. Serre-Tate Local Moduli, *Surfaces Algébriques*, Séminaire de Géométrie Algébrique d'Orsay, 138-202, 1976-78.

[6] N. Katz and B. Mazur. *Arithmetic Moduli of Elliptic Curves*, Annals of Mathematics Studies, Princeton University Press, 1985.

[7] J. Lubin, J.-P. Serre and J. Tate. Elliptic curves and formal groups by J. Lubin, J.-P. Serre and J. Tate, Lecture notes prepared in connection with the seminars held

at the Summer Institute on Algebraic Geometry, Whitney Estate, Woods Hole, Massachusetts, July 6-July 31, 1964.

[8] W. Messing. *The Crystals Associated to Barsotti-Tate Groups, With Applications to Abelian Schemes*, Springer-Verlag, 1972.

[9] J.-P. Serre. *Local Fields*, Springer-Verlag, 1980.

[10] J. Tate. Finite Flat Group Schemes, *Modular Forms and Fermat's Last Theorem*, 121-154, Springer, 1997.

[11] J. Tate. p-Divisible Groups, *Proceedings of a conference on local fields*, 158-183, Driebergen, 1966.